

New quantum codes from dual-containing cyclic codes over finite rings

Yongsheng Tang¹, Shixin Zhu², Xiaoshan Kai², Jian Ding³

Abstract Let $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$, where \mathbb{F}_{2^m} is the finite field with 2^m elements, m is a positive integer, and u is an indeterminate with $u^{k+1} = 0$. In this paper, we propose the constructions of two new families of quantum codes obtained from dual-containing cyclic codes of odd length over R . A new Gray map over R is defined and a sufficient and necessary condition for the existence of dual-containing cyclic codes over R is given. A new family of 2^m -ary quantum codes is obtained via the Gray map and the Calderbank-Shor-Steane construction from dual-containing cyclic codes over R . In particular, a new family of binary quantum codes is obtained via the Gray map, the trace map and the Calderbank-Shor-Steane construction from dual-containing cyclic codes over R .

Key words Quantum codes; dual-containing cyclic codes; Gray map; trace map

1 Introduction

Quantum codes play an important role not only in quantum communication but also in quantum computation. Since quantum codes provide a guarantee for quantum computation and quantum communication, the construction of quantum codes with good parameters has been an important topic in quantum information. After the work of Calderbank et al.^[1] gave a thorough discussion of the principles of quantum codes, the most of the constructions of quantum codes were transformed to construct self-orthogonal (or dual-containing) classical codes. Many works have been done for constructing good binary quantum codes by using classical codes, such as Bose-Chaudhuri-Hocquenghem (BCH) codes, Reed-Solomon codes, Reed-Muller codes and algebraic geometric codes (see Refs. 2-6). Some of these constructions were generalized to the case of nonbinary quantum codes, since nonbinary quantum codes can be applied in fault-tolerant quantum computation. Ashikhmin and Knill^[7] constructed nonbinary quantum codes by using classical self-orthogonal codes. Ketkar et al.^[8] constructed many families of nonbinary quantum codes, including quantum Hamming codes, quadratic residue codes, quantum Melas codes, quantum BCH codes, and quantum character codes. La Guardia^[9,10] constructed new families of nonbinary quantum codes derived from classical BCH codes.

Cyclic codes are a well-studied class of codes that have play an essential role in both theory and practice. Cyclic codes have also extensively been used to construct quantum codes. Thangaraj and McLaughlin^[11] constructed quantum codes from cyclic codes over $\text{GF}(4^m)$. R.

1.School of Mathematics and Statistics, Hefei Normal University, Hefei, Anhui 230601, China.

2.School of Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China.

3.Department of Common Course, Anhui Xinhua University, Hefei, Anhui 230088, China.

Email: ysh_tang@163.com(Y.Tang), sxinzhu@tom.com(S.Zhu), kxs6@sina.com(X.Kai), 415134412@qq.com(J.Ding).

*This research is supported by National Natural Science Funds of China (Nos. 61370089 and 61572168), Natural Science Foundation of Anhui Province (No. 1408085QF116), National Mobil Communications Research Laboratory, Southeast University(No. 2014D04), Colleges Outstanding Young Talents Program in 2014, Anhui Province (No. [2014]181), Anhui Province Natural Science Research (No. KJ2015A308) and Hefei Normal University Research Project (No. 2015JG09).

Li and X. Li^[12] constructed binary quantum codes from cyclic code of length $2^\alpha n$ with n odd and $n \leq 99$, and $\alpha \leq 2$. Qian et al.^[13] constructed quantum codes from quasi-cyclic codes. Kai et al.^[14–16] constructed many classes of quantum codes from negacyclic and constacyclic codes. Wang and Zhu^[17] constructed non-binary quantum from repeated-root cyclic codes. Chen et al.^[18] constructed quantum codes from constacyclic codes.

Recently, many good quantum codes have been constructed from cyclic codes over finite rings. Qian and Zhang^[19] constructed quantum codes from cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Kai and Zhu^[20] constructed quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Guenda and Gulliver^[21] constructed quantum codes from linear codes over finite commutative Frobenius rings. Ashraf and Mohammad^[22] constructed quantum codes from cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$.

The purpose of this paper is to construct two new families of quantum codes by taking advantage of dual-containing cyclic codes over the finite commutative ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$. This paper is organized as follows. In Section 2, some definitions and notations about linear and cyclic codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ are provided. In Section 3, a new Gray map on $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ is defined. In Section 4, a necessary and sufficient condition for the existence of dual-containing cyclic codes is obtained and a new family of 2^m -ary quantum codes is constructed. In Section 5, a new family of binary quantum codes is constructed. Section 6 concludes the paper.

2 Preliminaries

Let \mathbb{F}_{2^m} be the finite field with 2^m elements and R be the commutative ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m} \simeq \mathbb{F}_{2^m}[u]/(u^{k+1})$. The ring R is a finite chain ring whose ideals can be linearly ordered by inclusion; that is, $0 = u^{k+1}R \subset u^kR \subset \cdots \subset u^2R \subset uR \subset R$. The ring R is given by the obvious addition and multiplication with $u^{k+1} = 0$. The units of R are the elements $a \in R$ such that $a \not\equiv 0 \pmod{u}$ and the residue field is $R/uR \simeq \mathbb{F}_{2^m}$. A code of length n over R is a nonempty subset of R^n , and a code is linear over R if it is an R -submodule of R^n . Given two vectors $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$, and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1}) \in R^n$, their Euclidean inner product is defined as

$$\mathbf{x} \cdot \mathbf{y} = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1} \in R.$$

The vectors \mathbf{x} and \mathbf{y} are called orthogonal with respect to the Euclidean inner product if $\mathbf{x} \cdot \mathbf{y} = 0$. For a linear code \mathcal{C} of length n , the Euclidean dual code of \mathcal{C} is defined as

$$\mathcal{C}^\perp = \{\mathbf{x} \in R^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in \mathcal{C}\}.$$

A linear code \mathcal{C} of length n over R is called dual-containing if $\mathcal{C}^\perp \subseteq \mathcal{C}$, and it is called self-dual if $\mathcal{C} = \mathcal{C}^\perp$. Two codes are equivalent if one can be obtained from the other by permuting the coordinates. Any code over R is permutation equivalent to a code \mathcal{C} with generator matrix of the form

$$G = \begin{pmatrix} I_{l_0} & A_{1,1} & A_{1,2} & A_{1,3} & \cdots & A_{1,k-1} & A_{1,k} \\ 0 & uI_{l_1} & uA_{2,1} & uA_{2,2} & \cdots & uA_{2,k-1} & uA_{2,k} \\ 0 & 0 & u^2I_{l_2} & u^2A_{3,1} & \cdots & u^2A_{3,k-1} & u^2A_{3,k} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^kI_{l_k} & u^kA_{k,1} \end{pmatrix},$$

where l_i are all positive integers, $A_{i,j}$ are all matrices over R . Then \mathcal{C} is an abelian group of type $\{l_0, l_1, \dots, l_k\}$, \mathcal{C} contains $(2^{(k+1)m})^{l_0} (2^{km})^{l_1} \cdots (2^m)^{l_k}$ codewords, and \mathcal{C} is a free R -module if

and only if $l_1 = l_2 = \dots = l_k = 0$. A linear code \mathcal{C} of length n over R is called cyclic if it is invariant under the cyclic shift τ of R^n :

$$\tau(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2}).$$

Each codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$, and the code \mathcal{C} is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $R[x]/\langle x^n - 1 \rangle$, $xc(x)$ corresponds to a cyclic shift of $c(x)$. It is well known that a linear code \mathcal{C} of length n over R is cyclic if and only if \mathcal{C} is an ideal of the quotient ring $R[x]/\langle x^n - 1 \rangle$. Throughout this paper, we assume that the length n is odd. It has been shown that the ring $R[x]/\langle x^n - 1 \rangle$ is a principal ideal ring.

3 Gray Map on R

Every element $c \in R$ can be written uniquely as

$$c = \beta_0(c) + u\beta_1(c) + \dots + u^k\beta_k(c),$$

where $\beta_i(c) \in \mathbb{F}_{2^m}$, for $i = 0, 1, \dots, k$. A new Gray map Φ on R is defined as

$$\Phi : R \rightarrow \mathbb{F}_{2^m}^{k+1},$$

$$\beta_0(c) + u\beta_1(c) + \dots + u^k\beta_k(c) \mapsto (\beta_k(c), \beta_k(c) + \beta_0(c), \beta_{k-1}(c) + \beta_0(c), \beta_{k-1}(c) + \beta_1(c), \dots, e(c)),$$

where

$$e(c) = \begin{cases} \beta_{t+1}(c) + \beta_t(c), & \text{if } k = 2t + 1, \\ \beta_t(c) + \beta_{t-1}(c), & \text{if } k = 2t. \end{cases}$$

The Gray weight w_G of $c \in R$ is defined to be the sum of the Hamming weight of $\Phi(c)$, i.e., $w_G(c) = w_H(\Phi(c))$. This extends to a weight function in R^n : if $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$, then $w_G(\mathbf{c}) = \sum_{i=0}^{n-1} w_G(c_i)$. The Gray distance $d_G(\mathbf{c}, \mathbf{c}')$ between any distinct vectors $\mathbf{c}, \mathbf{c}' \in R^n$ is defined to be $w_G(\mathbf{c} - \mathbf{c}')$. The minimum Gray distance of \mathcal{C} is the smallest nonzero Gray distance between all pairs of distinct codewords of \mathcal{C} . The minimum Gray weight of \mathcal{C} is the smallest nonzero Gray weight among all codewords of \mathcal{C} . If \mathcal{C} is linear, then the minimum Gray distance is the same as the minimum Gray weight. The Hamming weight w_H of a codeword $\mathbf{c} \in \mathcal{C}$ is the number of its nonzero components. The Hamming distance $d_H(\mathbf{c}, \mathbf{c}')$ between two codewords \mathbf{c} and \mathbf{c}' is the Hamming weight of the codeword $\mathbf{c} - \mathbf{c}'$. The minimum Hamming distance d_H of \mathcal{C} is defined as $\min\{d(\mathbf{c}, \mathbf{c}') | \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\}$. For any linear code, the minimum Hamming distance $d_H(\mathcal{C})$ of \mathcal{C} is its minimum Hamming weight. It is clear that Φ preserves linearity. The Gray map Φ can be extended to R^n in an obvious way and the extended Φ is a bijection from R^n to $\mathbb{F}_{2^m}^{(k+1)n}$.

The following property of the Gray map is obvious from the above definitions.

Proposition 3.1 *The map Φ is a weight preserving map from $(R^n, \text{Gray weight})$ to $(\mathbb{F}_{2^m}^{(k+1)n}, \text{Hamming weight})$ and a distance preserving map from $(R^n, \text{Gray distance})$ to $(\mathbb{F}_{2^m}^{(k+1)n}, \text{Hamming distance})$.*

Proposition 3.2 *Let \mathcal{C} be a linear code of length n and type $\{l_0, l_1, \dots, l_k\}$ over R , and let \mathcal{C}^\perp be the dual of the code \mathcal{C} . Then*

$$\Phi(\mathcal{C})^\perp = \Phi(\mathcal{C}^\perp).$$

Proof Let $c_1 = \beta_0(c_1) + u\beta_1(c_1) + \dots + u^k\beta_k(c_1) \in \mathcal{C}$, $c_2 = \beta_0(c_2) + u\beta_1(c_2) + \dots + u^k\beta_k(c_2) \in \mathcal{C}^\perp$. Then $c_1 \cdot c_2 = 0$; that is, $\beta_0(c_1)\beta_0(c_2) + \beta_1(c_1)\beta_0(c_2) + \beta_0(c_1)\beta_1(c_2) + \dots + \sum_{i=0}^t \beta_i(c_1)\beta_{t-i}(c_2) = 0$, for $t = 0, 1, \dots, k$. Therefore

$$\begin{aligned} \Phi(c_1) \cdot \Phi(c_2) &= (\beta_k(c_1), \beta_k(c_1) + \beta_0(c_1), \beta_{k-1}(c_1) + \beta_0(c_1), \beta_{k-1}(c_1) + \beta_1(c_1), \dots, e(c_1)) \\ &\quad \cdot (\beta_k(c_2), \beta_k(c_2) + \beta_0(c_2), \beta_{k-1}(c_2) + \beta_0(c_2), \beta_{k-1}(c_2) + \beta_1(c_2), \dots, e(c_2)) \\ &= \sum_{i=0}^k \beta_i(c_1)\beta_{k-i}(c_2) + \sum_{i=0}^{k-1} \beta_i(c_1)\beta_{k-1-i}(c_2) \\ &= 0. \end{aligned}$$

Since Φ is a bijection, it follows that $\Phi(\mathcal{C}^\perp) \subseteq \Phi(\mathcal{C})^\perp$. Now it is enough to show that the two sets have the same cardinality. Suppose \mathcal{C} is a linear code of length n and type $\{l_0, l_1, \dots, l_k\}$ over R , we can get $\Phi(\mathcal{C})$ is a $[(k+1)n, (k+1)l_0 + kl_1 + \dots + l_k]$ -linear code over \mathbb{F}_{2^m} . This implies that $\Phi(\mathcal{C})^\perp$ is a $[(k+1)n, (k+1)n - ((k+1)l_0 + kl_1 + \dots + l_k)]$ -linear code over \mathbb{F}_{2^m} . Therefore, $|\Phi(\mathcal{C})^\perp| = 2^{m((k+1)n - ((k+1)l_0 + kl_1 + \dots + l_k))}$. Since Φ is a bijection, then $|\Phi(\mathcal{C}^\perp)| = |\mathcal{C}^\perp| = 2^{m((k+1)n - ((k+1)l_0 + kl_1 + \dots + l_k))}$. Hence $|\Phi(\mathcal{C})^\perp| = |\Phi(\mathcal{C}^\perp)|$. ■

4 Code Construction I

In this section, we construct a new family of 2^m -ary quantum codes by using dual-containing cyclic codes of odd length over R . A fundamental link between linear codes and quantum codes is given by the Calderbank-Shor-Steane (CSS) construction. We first recall some definitions and notations.

Let $f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_0$ be a polynomial in $R[x]$. Define the reciprocal polynomial of $f(x)$ as $f^*(x) = x^k f(x^{-1})$, i.e., $f^*(x) = a_0 x^k + a_1 x^{k-1} + \dots + a_k$. Obviously, $(f^*(x))^* = f(x)$ and $(f(x)g(x))^* = f^*(x)g^*(x)$. If there exists a unit ε in R such that $f(x) = \varepsilon f^*(x)$, then $f(x)$ is called self-reciprocal over R ; otherwise, $f(x)$ is called non self-reciprocal over R . If $f(x)$ is an irreducible and non self-reciprocal divisor of $x^n - 1$, then $f^*(x)$ is also an irreducible and non self-reciprocal divisor of $x^n - 1$. Such $f(x)$ and $f^*(x)$ are called irreducible reciprocal polynomial pairs. Let $f(x)$ be a monic factor of $x^n - 1$, then we denote $\widehat{f}(x) = \frac{x^n - 1}{f(x)}$. Every cyclic code \mathcal{C} has generator polynomial in the following form.

Theorem 4.1^[23] *Let \mathcal{C} be a cyclic code over R of length n . Then there exists a unique family of monic pairwise coprime polynomials $f_0(x), f_1(x), f_2(x), \dots, f_{k+1}(x)$ in $R[x]$ such that $f_0(x)f_1(x)f_2(x) \cdots f_{k+1}(x) = x^n - 1$ and*

$$\mathcal{C} = \langle \widehat{f}_1(x), u\widehat{f}_2(x), u^2\widehat{f}_3(x), \dots, u^k\widehat{f}_{k+1}(x) \rangle$$

with $|\mathcal{C}| = 2^{m(\sum_{i=0}^k (k+1-i)\deg f_{i+1}(x))}$. Moreover

$$\mathcal{C}^\perp = \langle \widehat{f}_0^*(x), u\widehat{f}_{k+1}^*(x), u^2\widehat{f}_k^*(x), \dots, u^k\widehat{f}_2^*(x) \rangle$$

with $|\mathcal{C}^\perp| = 2^{m(\sum_{i=0}^{k+1} \deg f_{i+1}(x))}$.

Now we obtain a sufficient and necessary condition for the existence of dual-containing cyclic codes over R by using generator polynomials of cyclic codes over R .

Theorem 4.2 *Let \mathcal{C} be a cyclic code over R of length n . Then there exists a unique family of monic pairwise coprime polynomials $f_0(x), f_1(x), f_2(x), \dots, f_{k+1}(x)$ in $R[x]$ such that $f_0(x)f_1(x)f_2(x) \cdots f_{k+1}(x) = x^n - 1$ and*

$$\mathcal{C} = \langle \widehat{f}_1(x), u\widehat{f}_2(x), u^2\widehat{f}_3(x), \dots, u^k\widehat{f}_{k+1}(x) \rangle.$$

Let $r_i(x)$ be the product of irreducible and non self-reciprocal divisors in $f_i(x)$ which do not occur in pairs, for $i = 2, 3, \dots, k+1$. Then $\mathcal{C}^\perp \subseteq \mathcal{C}$ if and only if $(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)) | f_1^*(x)$.

Proof By Theorem 4.1, we obtain

$$\mathcal{C}^\perp = \langle \widehat{f}_0^*(x), u\widehat{f}_{k+1}^*(x), u^2\widehat{f}_k^*(x), \dots, u^k\widehat{f}_2^*(x) \rangle.$$

If $\mathcal{C}^\perp \subseteq \mathcal{C}$, then there exists $a(x) \in \mathbb{F}_{2^m}[x]$ such that $\widehat{f}_0^*(x) = \widehat{f}_1(x)a(x)$. Let $f_i(x) = b_i(x)r_i(x)$, where $b_i(x) = \varepsilon_i b_i^*(x)$ with $\varepsilon_i \in \mathbb{F}_{2^m}^*$ for $i = 2, 3, \dots, k+1$. Then

$$f_1^*(x)b_2^*(x)r_2^*(x) \cdots b_{k+1}^*(x)r_{k+1}^*(x) = f_0(x)b_2(x)r_2(x) \cdots b_{k+1}(x)r_{k+1}(x)a(x).$$

For $i = 2, 3, \dots, k+1$, each $r_i(x)$ is not a self-reciprocal polynomial, then $r_i(x)$ and $b_i^*(x)r_i^*(x)$ are relatively coprime. Therefore, $r_i(x) | f_1^*(x)$, for $i = 2, 3, \dots, k+1$. Since distinct $r_i(x)$ are relatively coprime, for $i = 2, 3, \dots, k+1$, it follows that $(r_2(x)r_3(x) \cdots r_{k+1}(x)) | f_1^*(x)$. We know that $f_1^*(x)f_2^*(x) \cdots f_{k+1}^*(x)f_1(x) = f_0(x)f_1(x)f_2(x) \cdots f_{k+1}(x)a(x) = -f_0^*(x)f_1^*(x)f_2^*(x) \cdots f_{k+1}^*(x)a(x)$, then $f_0(x) | f_1^*(x)$. Since $f_0(x)$ and each $r_i(x)$ are relatively coprime, we have $(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)) | f_1^*(x)$.

On the other hand, if $(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)) | f_1^*(x)$, there exists $m(x) \in \mathbb{F}_{2^m}[x]$ such that $f_1^*(x) = f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)m(x)$. Since $f_1(x)$ and $f_{k+1}(x)$ are relatively coprime, there exist $s(x)$ and $t(x)$ in $\mathbb{F}_{2^m}[x]$ such that $f_1(x)s(x) + f_{k+1}(x)t(x) = 1$. Therefore

$$\begin{aligned} u\widehat{f}_{k+1}^*(x) &= uf_0^*(x)f_1^*(x)f_2^*(x) \cdots f_k^*(x)(f_1(x)s(x) + f_{k+1}(x)t(x)) \\ &= uf_0^*(x)(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)m(x))(b_2(x)r_2(x) \cdots b_k(x)r_k(x))^* f_1(x)s(x) \\ &\quad + uf_0^*(x)(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)m(x))(b_2(x)r_2(x) \cdots b_k(x)r_k(x))^* f_{k+1}(x)t(x) \\ &= u\varepsilon_2 \cdots \varepsilon_k f_0(x)f_1(x)f_2(x) \cdots f_k(x)f_0^*(x)r_2^*(x) \cdots r_k^*(x)r_{k+1}(x)m(x)s(x) \\ &\quad + u\varepsilon_2 \cdots \varepsilon_k f_0(x)f_2(x)f_3(x) \cdots f_{k+1}(x)f_0^*(x)r_2^*(x) \cdots r_k^*(x)r_{k+1}(x)m(x)t(x) \in \mathcal{C}. \end{aligned}$$

Similarly, we can prove that $u^2\widehat{f}_k^*(x) \in \mathcal{C}, \dots, u^k\widehat{f}_2^*(x) \in \mathcal{C}$. Furthermore

$$\begin{aligned} \widehat{f}_0^*(x) &= (f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x)m(x))(b_2(x)r_2(x) \cdots b_{k+1}(x)r_{k+1}(x))^* \\ &= \varepsilon_2 \cdots \varepsilon_{k+1} f_0(x)f_2(x) \cdots f_{k+1}(x)m(x)r_2^*(x)r_3^*(x) \cdots r_{k+1}^*(x) \in \mathcal{C}. \end{aligned}$$

Hence $\mathcal{C}^\perp \subseteq \mathcal{C}$. This completes the proof. \blacksquare

An important application of dual-containing codes is the constructions of quantum codes. We denote by $[[n, l, d]]_q$ a q -ary quantum code for n qubits having q^l codewords and minimum

distance d . It is well known that quantum codes with parameters $[[n, l, d]]_q$ must satisfy the quantum Singleton bound: $l \leq n - 2d + 2$ (see Refs. [14-16]). A quantum code achieving this bound is called a quantum maximum-distance-separable (MDS) code. Quantum MDS codes are optimal. A fundamental link between linear codes and quantum codes is given by the CSS construction.

Theorem 4.3^[1] (*CSS construction*) *Let \mathcal{C} and \mathcal{C}' be two linear codes over \mathbb{F}_q with parameters $[n, t_1, d_1]_q$ and $[n, t_2, d_2]_q$. If $\mathcal{C}^\perp \subseteq \mathcal{C}'$, then there exists a q -ary quantum code with parameters $[[n, t_1 + t_2 - n, \min\{d_1, d_2\}]]_q$. Especially, if $\mathcal{C}^\perp \subseteq \mathcal{C}$, then there exists a q -ary quantum code with parameters $[[n, 2t_1 - n, d_1]]_q$.*

Now, based on dual-containing cyclic codes over R , the Gray map and the CSS construction, we construct a new family of 2^m -ary quantum codes. From Theorems 4.2 and 4.3, we directly get the following results.

Theorem 4.4 *Let*

$$\mathcal{C} = \langle \widehat{f}_1(x), u\widehat{f}_2(x), u^2\widehat{f}_3(x), \dots, u^k\widehat{f}_{k+1}(x) \rangle$$

be a cyclic code over R of length n , type $\{l_0, l_1, \dots, l_k\}$ and the minimum Gray distance d_G , where $f_0(x), f_1(x), f_2(x), \dots, f_{k+1}(x)$ are a unique family of monic pairwise coprime polynomials in $R[x]$ and $f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x) = x^n - 1$. If there exist $r_i(x)$ are the product of irreducible and non self-reciprocal divisors in $f_i(x)$ which do not occur in pairs, for $i = 2, 3, \dots, k+1$ and $(f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x))|f_1^(x)$, then $\mathcal{C}^\perp \subseteq \mathcal{C}$, and there exists a 2^m -ary quantum code with parameters $[[(k+1)n, 2((k+1)l_0 + kl_1 + \dots + l_k) - (k+1)n, d_G]]$.*

Let us use the following examples to illuminate the method of the above construction.

Example 4.5 Consider a cyclic code with length 15 over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$.

Note that

$$x^{15} - 1 = (x - 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$. Taking $f_1(x) = 1, f_2(x) = (x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1), f_3(x) = x^4 + x^3 + 1, f_4(x) = 1, f_5(x) = x - 1$. Then

$$\mathcal{C} = \langle \widehat{f}_1(x), u\widehat{f}_2(x), u^2\widehat{f}_3(x), u^3\widehat{f}_4(x) \rangle$$

is a cyclic code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ of length 15, type $\{10, 4, 0, 1\}$, the minimum Gray distance 4 and $\mathcal{C}^\perp \subseteq \mathcal{C}$. By Theorem 4.4, we can obtain a $Q = [[60, 46, 4]]_2$ quantum code, which meets the bound in Ref. 24. Thus, the obtained quantum code is optimal.

5 Code Construction II

In this section, we will give another method to construct quantum codes by using dual-containing cyclic codes of odd length over R . We recall some definitions on the finite field \mathbb{F}_{2^m} firstly.

Definition 5.1^[25]. *Let $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a basis for \mathbb{F}_{2^m} over \mathbb{F}_2 . We call that B is a Trace Orthogonal Basis (TOB), if we have*

$$\text{Tr}(\alpha_i \alpha_j) = \begin{cases} 0, & \text{if } \alpha_i \neq \alpha_j, \\ 1, & \text{if } \alpha_i = \alpha_j, \end{cases}$$

where Tr is the usual Trace function from \mathbb{F}_{2^m} to \mathbb{F}_2 .

In this work, we let $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a self-dual basis for \mathbb{F}_{2^m} over \mathbb{F}_2 . Let \mathcal{C}' be a cyclic code over \mathbb{F}_{2^m} of length N . For $\mathbf{c}' = (c'_1, c'_2, \dots, c'_N)$. Define a map φ by

$$\varphi : \mathbb{F}_{2^m}^N \rightarrow \mathbb{F}_2^{mN},$$

$$(c'_1, c'_2, \dots, c'_N) \mapsto (c_{11}, c_{21}, \dots, c_{N1}, c_{12}, c_{22}, \dots, c_{N2}, \dots, c_{1m}, c_{2m}, \dots, c_{Nm}),$$

where $c'_i = \sum_{j=1}^m c_{ij} \alpha_j$ for $i = 1, 2, \dots, N$ and $c_{ij} \in \mathbb{F}_2$. Let $\mathbf{a} \in \mathbb{F}_2^{mN}$, with

$$\mathbf{a} = (a_{11}, a_{21}, \dots, a_{N1}, a_{12}, a_{22}, \dots, a_{N2}, \dots, a_{1m}, a_{2m}, \dots, a_{Nm}) = (a^{(1)} | \dots | a^{(m)}),$$

where $a^{(i)} \in \mathbb{F}_2^N$, for $i = 1, 2, \dots, m$. Let $\sigma^{\otimes(m)}$ be the map from \mathbb{F}_2^{mN} to \mathbb{F}_2^{mN} given by

$$\sigma^{\otimes(m)}(\mathbf{a}) = (\tau(a^{(1)}) | \dots | \tau(a^{(m)})),$$

where τ is the usual cyclic shifts defined in Section 2 on \mathbb{F}_2 . A code C of length mN over \mathbb{F}_2 , if $\sigma^{\otimes(m)}(C) = C$, then the code C is said to be a quasi-cyclic code of index m over \mathbb{F}_2 .

Now we need the following theorems for constructing a new family binary quantum codes from dual-containing cyclic codes of odd length over R .

Theorem 5.2^[13] *Let \mathcal{C} be a cyclic codes over \mathbb{F}_{2^m} with parameters $[N, t, d]_{2^m}$. Then $\varphi(\mathcal{C})$ is a quasi-cyclic code of index m with parameters $[mN, mt, d' \geq d]_2$.*

Theorem 5.3 *Let \mathcal{C} be a cyclic code over R of length n , type $\{l_0, l_1, \dots, l_k\}$, the minimum Gray distance d_G and $\mathcal{C}^\perp \subseteq \mathcal{C}$. Then $\varphi \circ \Phi(\mathcal{C})$ is a quasi-cyclic code of index m with parameters $[(k+1)mn, m((k+1)l_0 + kl_1 + \dots + l_k), d' \geq d_G]_2$ and $\varphi \circ \Phi(\mathcal{C}^\perp) \subseteq \varphi \circ \Phi(\mathcal{C})$, where \circ means the composition of maps.*

Proof Since \mathcal{C} is a cyclic code over R of length n , type $\{l_0, l_1, \dots, l_k\}$, and the minimum Gray distance d_G , $\Phi(\mathcal{C})$ is a cyclic code \mathbb{F}_{2^m} with parameters $[(k+1)n, (k+1)l_0 + kl_1 + \dots + l_k, d_G]_{2^m}$. By Theorem 5.2, we obtain that $\varphi \circ \Phi(\mathcal{C})$ is a quasi-cyclic code of index m with parameters $[(k+1)mn, m((k+1)l_0 + kl_1 + \dots + l_k), d' \geq d_G]_2$. Now, we show that $\varphi \circ \Phi(\mathcal{C}^\perp) \subseteq \varphi \circ \Phi(\mathcal{C})$. Let $c_1 = \beta_0(c_1) + u\beta_1(c_1) + \dots + u^k\beta_k(c_1)$ and $c_2 = \beta_0(c_2) + u\beta_1(c_2) + \dots + u^k\beta_k(c_2)$ be any two elements in \mathcal{C} , where $\beta_i(c_1) = a_{i1}\alpha_1 + a_{i2}\alpha_2 + \dots + a_{im}\alpha_m$ and $\beta_i(c_2) = b_{i1}\alpha_1 + b_{i2}\alpha_2 + \dots + b_{im}\alpha_m$, with $a_{ij}, b_{ij} \in \mathbb{F}_2$ for $i, j = 0, 1, \dots, k$. Since $\mathcal{C}^\perp \subseteq \mathcal{C}$ and Φ is a bijection, it follows that $\Phi(\mathcal{C}^\perp) \subseteq \Phi(\mathcal{C})$. Therefore, $\sum_{i=0}^t \beta_i(c_1)\beta_{t-i}(c_2) = 0$, for $t = 0, 1, \dots, k$; that is, $\sum_{i,\mu,\lambda} a_{i,\mu} b_{t-i,\lambda} \alpha_\mu \alpha_\lambda = 0$, for $t = 0, 1, \dots, k$ and $\mu, \lambda = 1, 2, \dots, m$. Taking the trace over \mathbb{F}_2 , we get

$$\sum_{i,\mu,\lambda} a_{i,\mu} b_{t-i,\lambda} \text{Tr}(\alpha_\mu \alpha_\lambda) = 0.$$

Since $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ is a self-dual basis for \mathbb{F}_{2^m} over \mathbb{F}_2 , we get that $\text{Tr}(\alpha_\lambda^2) = 1$ for $\mu = \lambda$ and $\text{Tr}(\alpha_\mu \alpha_\lambda) = 0$ for $\mu \neq \lambda$. Therefore, $\sum_{i,\lambda} a_{i,\lambda} b_{t-i,\lambda} = 0$. This completes the proof. \blacksquare

Now, based on dual-containing cyclic codes over R , the Gray map and the trace map, we construct a new family of binary quantum codes by using the CSS construction. From Theorems 4.2 and 5.3, we directly get the following results.

Theorem 5.4 *Let*

$$\mathcal{C} = \langle \widehat{f}_1(x), u\widehat{f}_2(x), u^2\widehat{f}_3(x), \dots, u^k\widehat{f}_{k+1}(x) \rangle$$

be a cyclic code over R of length n , type $\{l_0, l_1, \dots, l_k\}$ and the minimum Gray distance d_G , where $f_0(x), f_1(x), f_2(x), \dots, f_{k+1}(x)$ are a unique family of monic pairwise coprime polynomials in $R[x]$ and $f_0(x)f_1(x)f_2(x) \cdots f_{k+1}(x) = x^n - 1$. Let $r_i(x)$ be the product of irreducible and non self-reciprocal divisors in $f_i(x)$ which do not occur in pairs, for $i = 2, 3, \dots, k+1$ and $(f_0(x)r_2(x)r_3(x) \cdots r_{k+1}(x))|f_1^(x)$. Then $\mathcal{C}^\perp \subseteq \mathcal{C}$. Hence, there exists a binary quantum code with parameters $[[(k+1)mn, 2m((k+1)l_0 + kl_1 + \cdots + l_k) - (k+1)mn, \geq d_G]]$.*

In the following, we give an example for construction a 4-ary quantum code and a binary quantum code by taking advantage of a dual-containing cyclic code over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$.

Example 5.5 Let $\mathbb{F}_{2^2} = \{0, 1, \omega, \omega^2\}$ be a finite field with four elements, where $\omega^2 = \omega + 1$. Consider a cyclic code with length 21 over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$.

Note that

$$x^{21} - 1 = (x - 1)(x + \omega)(x + \omega^2)(x^3 + x + 1)(x^3 + x^2 + 1)(x^3 + \omega x + 1)(x^3 + \omega x^2 + 1)(x^3 + \omega^2 x + 1)(x^3 + \omega^2 x^2 + 1)$$

over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$. Let $f(x) = x^3 + \omega^2 x + 1, g(x) = (x - 1)(x + \omega)(x + \omega^2)(x^3 + x^2 + 1)(x^3 + \omega x + 1)(x^3 + x + 1)(x^3 + \omega x^2 + 1)(x^3 + \omega^2 x^2 + 1), h(x) = (x - 1)$. Then

$$\mathcal{C} = \langle f(x)h(x), uf(x)g(x) \rangle$$

is a cyclic code over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$ of length 21, type $\{20, 0, 1\}$, the minimum Gray distance 2 and $\mathcal{C} \subseteq \mathcal{C}^\perp$. By Theorem 4.4, we can obtain a $Q' = [[42, 40, 2]]_4$ quantum code, which is a quantum MDS code. Thus, the obtained quaternary quantum code is optimal. On the other hand, we know that $B = \{1, \omega\}$ is a self-dual basis for \mathbb{F}_{2^2} over \mathbb{F}_2 . By Theorem 5.4, we can obtain a $Q'' = [[84, 80, d'' \geq 2]]_2$ quantum code, which meets the bound in Ref.[24]. Thus, the obtained binary quantum code is good.

We list some quantum codes which can be constructed starting from dual-containing cyclic codes over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$ in Table I. Compared the parameters of quantum codes available in Refs. 12, 24, 26-28, we find that most of our obtained quantum codes have good parameters.

TABLE I Quantum codes from dual-containing cyclic codes over $\mathbb{F}_{2^2} + u\mathbb{F}_{2^2}$

Length	Minimum Gray distance	Type	Quantum code I	Quantum code II
7	2	$\{6, 0, 1\}$	$[[14, 12, 2]]_4$	$[[28, 24, d' \geq 2]]_2$
17	4	$\{13, 0, 4\}$	$[[34, 26, 4]]_4$	$[[68, 52, d' \geq 4]]_2$
31	4	$\{25, 0, 6\}$	$[[62, 50, 4]]_4$	$[[124, 100, d' \geq 4]]_2$
35	4	$\{30, 0, 5\}$	$[[70, 60, 4]]_4$	$[[140, 120, d' \geq 4]]_2$
43	5	$\{36, 0, 0\}$	$[[86, 78, 5]]_4$	$[[172, 156, d' \geq 5]]_2$

Remark 5.5 Compared with previously known quantum codes in Refs. 12, 24, 26-28, some of our obtained quantum codes are optimal and new in Table I. For quaternary case, our obtained quantum codes $[[14, 12, 2]]_4$ and $[[86, 78, 5]]_4$ are quantum MDS codes. Thus, they are optimal. Comparing with the known quantum code $[[34, 24, 4]]_4$ given in Ref.26, our obtained quantum code $[[34, 26, 4]]_4$ is optimal and new. Comparing with the highest achievable minimum distance quantum codes $[[n, n - 12, 4]]_4$ given in Ref.27(Corollary 3.2), the obtained quantum code $[[62, 50, 4]]_4$ has the same parameters and the obtained quantum code $[[70, 60, 4]]_4$ is optimal and new. For binary case, we obtain the first three quantum codes, which nearly

meet the bound in Ref.24. Comparing with the known quantum code $[[143, 121, 3]]_2$ given in Ref.28, our obtained quantum code $[[140, 120, d' \geq 4]]_2$ is good. Furthermore, we obtain the quantum code $[[172, 156, d' \geq 5]]_2$. Comparing with the known quantum codes $[[170, 130, 5]]_2$ and $[[178, 154, 3]]_2$ given in Ref.12, our obtained quantum code is good. The example shows that optimal and new quantum codes also can be constructed from cyclic codes over finite rings.

6 Conclusion

Constructing quantum codes with good parameters has been an important topic in quantum information. Many good quantum codes were constructed from Hamming codes, BCH codes, Reed-Solomon codes, Reed-Muller codes and algebraic geometry codes. In this paper, two new families of quantum codes have been constructed by taking advantage of dual-containing cyclic codes over the finite ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$. The constructed quantum codes have good parameters. Furthermore, some of the constructed quantum codes are new. The results show that cyclic codes over finite rings are also a good resource of constructing quantum codes. Our constructions are almost theoretical, while it is very significant to discuss the implementation of these constructions in hardware. It would be very interesting to find a practical physical implementation for a quantum code from finite rings.

References

References

- [1] A.R.Calderbank, E.M.Rains, P.W.Shor, N.J.A.Sloane, Quantum error correction via codes over $\text{GF}(4)$, IEEE Trans. Inform. Theory 44 (1998) 1369-1387.
- [2] S.A.Aly, A.Klappenecker, P.K.Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inform. Theory 53 (2007) 1183-1188.
- [3] Z.Li, L.Xing, X.Wang, Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance separable codes, Phys. Rev. A, 77(2008) 012308(1-4).
- [4] A.M.Steane, Quantum Reed-Muller codes, IEEE Trans. Inform. Theory 45 (1999) 1701-1703.
- [5] H.Chen, S.Ling, C.Xing, Quantum codes from concatenated algebraic geometric codes, IEEE Trans. Inform. Theory 51 (2005) 2915-2920.
- [6] K.Feng, S.Ling, C.Xing, Asymptotic bounds on quantum codes from algebraic geometric codes, IEEE Trans. Inform. Theory 52 (2006) 986-991.
- [7] A.Ashikhmin, E.Knill, Nonbinary quantum stabilizer code, IEEE Trans. Inform. Theory 47 (2001) 3065-3072.
- [8] A.Ketkar, A.Klappenecker, S.Kumar, P.K.Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inform. Theory 52 (2006) 4892-4914.
- [9] G.G.La Guardia, R. Palazzo, Jr., Constructions of new families of nonbinary CSS codes, Discrete Math. 310 (2010) 2935-2945.

-
- [10] G.G. La Guardia, Constructions of new families of nonbinary quantum codes, *Phys. Rev. A* 80 (2009) 042331 (1-11).
 - [11] A.Thangaraj, S.W.McLaughlin, Quantum codes from cyclic codes over $\text{GF}(4^m)$, *IEEE Trans. Inform. Theory* 47 (2001) 1176-1178.
 - [12] R.Li, X.Li, Quantum codes constructed from binary cyclic codes, *International Journal of Quantum Information* 2(2004) 265-272.
 - [13] J.Qian, W.Ma, X.Wang, Quantum error-correcting codes from quasi-cyclic codes, *International Journal of Quantum Information* 6 (2008) 1263-1269.
 - [14] X.Kai, S.Zhu, New quantum MDS codes from negacyclic codes, *IEEE Trans. Inform. Theory* 59 (2013) 1193-1197.
 - [15] X. Kai, S. Zhu, Y.Tang, Quantum negacyclic codes, *Physical Review A* 88(2013)012326 (1-5).
 - [16] X.Kai, S.Zhu, P.Li, Constacyclic codes and some new quantum MDS codes, *IEEE Trans. Inform. Theory* 60 (2014) 2080-2085.
 - [17] L.Wang, S.Zhu, On non-binary quantum repeated-root cyclic codes, *International Journal of Quantum Information* 2 (2014) 265-272.
 - [18] B.Chen, S.Ling, G.Zhang, Application of constacyclic codes to quantum MDS codes, *IEEE Trans. Inform. Theory* 61 (2015) 1474-1484.
 - [19] J.Qian, W.Ma, W.Guo, Quantum codes from cyclic codes over finite rings, *International Journal of Quantum Information* 7 (2009) 1277-1283.
 - [20] X.Kai, S.Zhu, Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$, *International Journal of Quantum Information* 9 (2011) 689-700.
 - [21] K.Guenda, T.A.Gulliver, Quantum codes over rings, *International Journal of Quantum Information* 12 (2014) 1450020(1-11).
 - [22] M.Ashraf, G. Mohammad, Quantum codes from cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$, *International Journal of Quantum Information* 12 (2014) 1450042(1-8).
 - [23] H.Q.Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* 50 (2004) 1728-1744.
 - [24] M.Grassl, Bounds on the minimum distance of linear codes. <http://www.codetables.de>.
 - [25] F.J.Macwilliams, N.J.A.Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam New York, 1977.
 - [26] D.Bartoli, S.Marcugini, F. Pambianco, New quantum caps in $\text{PG}(4,4)$, *Journal of Combinatorial Designs* 20 (2012)448-466. see also arXiv:0905.1059v2
 - [27] R.Li, Q.Fu, L.Guo, X.Li, Construction of quantum caps in projective space $\text{PG}(r, 4)$ and quantum codes of distance 4, *Quantum Inf. Processing* 15 (2016) 689-720.
 - [28] Y.Edel's homepage, <http://www.mathi.uni-heidelberg.de/~yves>.